CLAIMS:

1. A computer comprising:

an interface adapted to couple with a dynamic database; and

processing circuitry configured to provide a first hash from digital data stored within a portion of the dynamic database at an initial moment in time, to provide a second hash from digital data stored within the portion of the dynamic database at a subsequent moment in time, and to compare the first hash and the second hash.

2. The computer according to claim 1 wherein the processing circuitry is configured to provide a digital signature using digital data stored within the portion of the dynamic database at the initial moment in time, and to provide the first hash using the digital signature.

3. The computer according to claim 2 wherein the processing circuitry is configured to decrypt the digital signature to provide the first hash.

4. The computer according to claim 2 wherein the processing circuitry is configured to decrypt the digital signature using a public key corresponding to a private key of an entity which provided the digital signature at the initial moment in time.

5. A system comprising:

storage circuitry configured to store digital data at least some of which dynamically changes with respect to time, and to store a digital signature generated using digital data stored within the storage circuitry at an initial moment in time; and

processing circuitry configured to provide a first hash from the digital signature, and to provide a second hash from digital data stored within the storage circuitry at a subsequent moment in time and corresponding to the digital data of the digital signature, and to compare the first hash and the second hash.

6. The system according to claim 5 wherein the digital data of the digital signature is stored within a portion of the storage circuitry at the initial moment of time and the digital data stored within a storage circuitry at the subsequent moment in time is stored in the portion of the storage circuitry.

7. The system according to claim 5 wherein the processing circuitry utilizes a public key corresponding to a private key of an entity which provided the digital signature at the initial moment in time to provide the first hash from the digital signature.

8. The system according to claim 5 wherein the storage circuitry comprises a relational database.

9. The system according to claim 5 wherein the storage circuitry is configured to store a static form of the digital data stored at the initial moment in time, and the processing circuitry is configured to provide the digital signature using the static form of the digital data, to provide a third hash from the static form of the digital data, and to compare the third hash with the first hash.

10. The system according to claim 5 wherein the storage circuitry is configured to store query information regarding storage of the digital data of the digital signature at the initial moment in time, and the processing circuitry is configured to use the query information to retrieve the digital data stored within the storage circuitry at the subsequent moment in time to provide the second hash.

11. A digital data system comprising:

storage circuitry configured to store digital data at least some of which dynamically changes with respect to time; and

processing circuitry configured to compare a first hash and a second hash, wherein the first hash corresponds to digital data stored within the storage circuitry at an initial moment in time and the second hash corresponds to digital data stored within the storage circuitry at a subsequent moment in time.

12. The system according to claim 11 wherein the digital data corresponding to the first hash is stored within a portion of the storage circuitry at the initial moment of time and the digital data stored within the storage circuitry at the subsequent moment in time is stored in the portion of the storage circuitry.

13. The system according to claim 11 wherein the processing circuitry is configured to provide a digital signature using the digital data stored within the dynamic database at the initial moment in time, and to provide the first hash using the digital signature.

14. The system according to claim 13 wherein the processing circuitry utilizes a public key corresponding to a private key of an entity which provided the digital signature at the initial moment in time to provide the first hash from the digital signature.

15. The system according to claim 13 wherein the storage circuitry is configured to store a static form of the digital data stored at the initial moment in time, and the processing circuitry is configured to provide the digital signature using the static form of the digital data, to provide a third hash from the static form of the digital data, and to compare the third hash with the first hash.

16. The system according to claim 11 wherein the storage circuitry comprises a relational database.

17. The system according to claim 11 wherein the storage circuitry is configured to store query information regarding storage of the digital data at the initial moment in time, and the processing circuitry is configured to use the query information to retrieve the digital data stored within the storage circuitry at the subsequent moment in time to provide the second hash.

18. A digital data storage system comprising:

a dynamic database containing a plurality of tables individually configured to store digital data;

a snapshot database configured to store a snapshot of digital data retrieved from at least one table of the dynamic database at an initial moment in time;

an approval database configured to store a digital signature of the snapshot; and

a client configured to provide the digital signature from the snapshot, to provide a first hash from the snapshot, to provide a second hash from the digital signature, to compare the first hash and the second hash, to provide a third hash from data stored within the at least one table of the dynamic database at a subsequent moment in time, and to compare the third hash and the second hash.

19. A data verification method comprising:

storing digital data at an initial moment in time within a dynamic database;

providing a first hash of the digital data stored at the initial moment in time;

providing a second hash of digital data within the dynamic database at a subsequent moment in time; and

comparing the first hash and the second hash.

20. The method according to claim 19 wherein storing comprises storing in a portion of the dynamic database, and the providing the second hash comprises providing using digital data stored in the portion at the subsequent moment in time.

21. The method according to claim 19 further comprising providing a digital signature using the digital data stored at the initial moment in time, and wherein the providing the first hash comprises providing using the digital signature.

22. The method according to claim 21 wherein the providing the first hash comprises providing using a public key which corresponds to a private key of an entity which provided the digital signature at the initial moment in time.

23. The method according to claim 19 wherein the storing comprises storing within a dynamic database comprising a relational database.

24. The method according to claim 19 further comprising:

storing a static form of the digital data stored at the initial moment in time;

providing a digital signature using the static form;

providing a third hash using the static form; and

comparing the third hash and the first hash.

25. The method according to claim 19 further comprising:

storing query information regarding the storing; and

retrieving digital data within the dynamic database at the subsequent moment in time using the query information.

26. A data verification method comprising:

providing digital data at an initial moment in time within a portion of a dynamic database;

storing a static form of the digital data stored at the initial moment in time within a static database;

providing a digital signature using the static form of the digital data;

providing a first hash of the digital data stored at the initial moment in time using the digital signature;

providing a second hash of the digital data stored at the initial moment in time using the static form of the digital data;

comparing the first hash and the second hash;

providing a third hash of digital data stored within the portion of the dynamic database at a subsequent moment in time; and

comparing the first hash and the third hash.

27. The method according to claim 26 wherein the providing the first hash comprises providing using a public key which corresponds to a private key of an entity which provided the digital signature.

28. The method according to claim 26 wherein the providing digital data at the initial moment in time comprises providing query information regarding storage of the digital data at the initial moment in time within the portion of the dynamic database, and wherein the providing the third hash comprises retrieving the digital data stored within the portion of the dynamic database using the query information.

29. The method according to claim 26 wherein the providing digital data comprises providing within a portion of a relational database.